GEOLOCATION TECHNOLOGY & PRIVACY,
VIRGINIA'S LEGISLATIVE REACTION TO UNITED STATES v. JONES

Remarks before the House Oversight and Government Reform Committee
Michael R. Doucette
Commonwealth's Attorney
City of Lynchburg, VA

Chairman Chaffetz, Ranking Member Cummings, members of the committee, my name is Michael Doucette and I am the elected Commonwealth's Attorney out of Lynchburg, Virginia. I am also currently a board member of the National District Attorneys Association (NDAA), the largest association representing the voice of prosecutors across the country. I appreciate the invitation to testify before you today to provide Virginia's perspective on the use of geolocation information and changes made after the United States v. Jones court decision.

2012

United States v. Jones was decided and announced by the United States Supreme Court on January 23, 2012. By that time, the last day for introducing bills for the 2012 Virginia General Assembly session had elapsed. Yet, many of us realized that we needed to do something

quickly and could not wait until the 2013 session. (Virginia has a part-time legislature, which meets only for either 6 weeks or 8 weeks in the winter.)

However, the rules of the General Assembly allow the Governor to request the introduction of a bill after the filing deadline. As a result, Governor Robert McDonnell's office convened a small group consisting of prosecutors, defense attorneys and law enforcement to draft a bill to allow for a search warrant specifically for the use of a GPS device.

One of the problems we had to deal with related to the use of a GPS device was how to satisfy the "particularity requirement" for a search warrant when the product of the proposed search is neither in a particular location nor is a particular item. Another problem dealt with providing service of the warrant on the target of the GPS warrant without tipping him off that he is under surveillance. It would do no good to serve a copy of the search warrant with the attached affidavit to the person to be surveilled, and then tell that person to go about his usual (criminal) activity. There was much frank discussion behind the scenes and a bill was ultimately crafted.

HB1298 (Delegate David Albo) was introduced in the House of Delegates on February 15, 2012 and SB685 (Senator Bryce Reeves *et al*) was introduced in the Senate on February 16, 2012. After the bill was slightly amended in both chambers, it passed and was signed by Governor McDonnell on April 5, 2012. Because the bill had an emergency clause, it went into effect immediately upon the Governor's signature.

The language as passed was this:

§ 19.2-56.2. Application for and issuance of search warrant for a tracking device; installation and use. —

A. As used in this section, unless the context requires a different meaning:

"Judicial officer" means a judge, magistrate, or other person authorized to issue criminal warrants.

"Law-enforcement officer" shall have the same meaning as in § 9.1-101.

"Tracking device" means an electronic or mechanical device that permits a person to remotely determine or track the position or movement of a person or object. "Tracking device" includes devices that store geographic data for subsequent access or analysis and devices that allow for the real-time monitoring of movement.

"Use of a tracking device" includes the installation, maintenance, and monitoring of a tracking device but does not include the interception of wire, electronic, or oral communications or the capture, collection, monitoring, or viewing of images.

B. A law-enforcement officer may apply for a search warrant from a judicial officer to permit the use of a tracking device. Each application for a search warrant authorizing the use of a tracking device shall be made in writing, upon oath or affirmation, to a judicial officer for the circuit in which the tracking device is to be installed, or where there is probable cause to believe the offense for which the tracking device is sought has been committed, is being committed, or will be committed.

The law-enforcement officer shall submit an affidavit, which may be filed by electronically transmitted (i) facsimile process or (ii) electronic record as defined in § 59.1-480, and shall include:

1. The identity of the applicant and the identity of the law-enforcement agency conducting the investigation;

2. The identity of the vehicle, container, item, or object to which, in which, or on which the tracking device is to be attached, placed, or otherwise installed; the name of the owner or possessor of the vehicle, container, item, or object described, if known; and the jurisdictional area in which the vehicle, container, item, or object described is expected to be found, if known;

3. Material facts constituting the probable cause for the issuance of the search warrant and alleging substantially the offense in relation to which such tracking device is to be used and a showing that probable cause exists that the information likely to be obtained will be evidence of the commission of such offense; and

4. The name of the county or city where there is probable cause to believe the offense for which the tracking device is sought has been committed, is being committed, or will be committed.

C. 1. If the judicial officer finds, based on the affidavit submitted, that there is probable cause to believe that a crime has been committed, is being committed, or will be committed and that there is probable cause to believe the information likely to be obtained from the use of the tracking device will be evidence of the commission of such offense, the judicial officer shall issue a search warrant authorizing the use of the tracking device. The search warrant shall authorize the use of the tracking device from within the Commonwealth to track a person or property for a reasonable period of time, not to exceed 30 days from the issuance of the search warrant. The search warrant shall authorize the collection of the tracking data contained in or obtained from the tracking device but shall not authorize the interception of wire, electronic, or oral communications or the capture, collection, monitoring, or viewing of images.

2. The affidavit shall be certified by the judicial officer who issues the search warrant and shall be delivered to and preserved as a record by the clerk of the circuit court of the county or city where there is probable cause to believe the offense for which the tracking

device has been sought has been committed, is being committed, or will be committed. The affidavit shall be delivered by the judicial officer in person; mailed by certified mail, return receipt requested; or delivered by electronically transmitted facsimile process or by use of filing and security procedures as defined in the Uniform Electronic Transactions Act (§ 59.1-479 et seq.) for transmitting signed documents.

3. By operation of law, the affidavit, search warrant, return, and any other related materials or pleadings shall be sealed. Upon motion of the Commonwealth or the owner or possessor of the vehicle, container, item, or object that was tracked, the circuit court may unseal such documents if it appears that the unsealing is consistent with the ends of justice or is necessary to reasonably inform such person of the nature of the evidence to be presented against him or to adequately prepare for his defense.

4. The circuit court may, for good cause shown, grant one or more extensions, not to exceed 30 days each.

D. 1. The search warrant shall command the law-enforcement officer to complete the installation authorized by the search warrant within 15 days after issuance of the search warrant.

2. The law-enforcement officer executing the search warrant shall enter on it the exact date and time the device was installed and the period during which it was used.

3. Law-enforcement officers shall be permitted to monitor the tracking device during the period authorized in the search warrant, unless the period is extended as provided for in this section.

4. Law-enforcement officers shall remove the tracking device as soon as practical, but not later than 10 days after the use of the tracking device has ended. Upon request, and for good cause shown, the circuit court may grant one or more extensions for such removal for a period not to exceed 10 days each.

5. In the event that law-enforcement officers are unable to remove the tracking device as required by subdivision 4, the law-enforcement officers shall disable the device, if possible, and all use of the tracking device shall cease.

6. Within 10 days after the use of the tracking device has ended, the executed search warrant shall be returned to the circuit court of the county or city where there is probable cause to believe the offense for which the tracking device has been sought has been committed, is being committed, or will be committed, as designated in the search warrant, where it shall be preserved as a record by the clerk of the circuit court.

E. Within 10 days after the use of the tracking device has ended, a copy of the executed search warrant shall be served on the person who was tracked and the person

whose property was tracked. Service may be accomplished by delivering a copy to the person who, or whose property, was tracked or by leaving a copy with any individual found at the person's usual place of abode who is a member of the person's family, other than a temporary sojourner or guest, and who is 16 years of age or older and by mailing a copy to the person's last known address. Upon request, and for good cause shown, the circuit court may grant one or more extensions for such service for a period not to exceed 30 days each. Good cause shall include, but not be limited to, a continuing criminal investigation, the potential for intimidation, the endangerment of an individual, or the preservation of evidence.

F. The disclosure or publication, without authorization of a circuit court, by a court officer, law-enforcement officer, or other person responsible for the administration of this section of the existence of a search warrant issued pursuant to this section, application for such search warrant, any affidavit filed in support of such warrant, or any return or data obtained as a result of such search warrant that is sealed by operation of law is punishable as a Class 1 misdemeanor.

There were several key components to this drafting. Perhaps the most important was the definitional section at the very beginning.

- The concern was how to issue a search warrant in one particular jurisdiction but allow it to be valid in any other jurisdiction to which the object (usually an automobile) travelled in the future. For standard search warrants, a search warrant is issued in the jurisdiction in which there is probable cause to believe that the evidence or contraband sought will be located at that static point in time when the warrant is executed.

  To address this issue, we defined "use of a tracking device" to include the "installation, maintenance and ***monitoring***" of that device. The body of the statute then went on to discuss the mechanics of how a law enforcement officer would obtain and execute a search warrant for the use of a tracking device.

- The elements for the warrant's affidavit include identifying the object to be tracked, the names of the owner or possessor of that object, the jurisdiction in which that object is expected to be found, and the facts establishing probable cause to believe information about a criminal offense will be obtained by tracking that object.

- The search warrant itself is valid for 30 days from issuance. Additional 30 extensions may only be issued by the circuit court (Virginia's trial court of record). The installation of the tracking device must be completed within 15 days of the issuance of the warrant. The device must be removed within 10 days after the use of the device has ended. If for some reason the device cannot be removed, law enforcement must disable it.

- Upon issuance, the warrant and supporting affidavit are automatically sealed by the circuit court. Either the prosecution or any owner or possessor of the object tracked

may move for unsealing. However, the warrant and affidavit must be served on the owner and the possessor, if different, within 10 days of the end of the use of the tracking device. Additional 30-day extensions of this service requirement may be granted by the circuit court if the investigation is still ongoing.

While we were not sure at the time that we were able to foresee all the problems of converting the general search warrant statute language to a GPS search warrant statute, it appears from the lack of any amendments to Section 19.2-56.2 since 2012 that we hit most of the high spots.

2014

Anticipating through legislation where we believed United States v. Jones might ultimately lead, in 2014 we amended VA Code §19.2-70.3 (Obtaining Records Concerning Electronic Communication Service or Remote Computing Service) to require a search warrant for the disclosure for up to 30 days of the ***real-time location data*** of any electronic device. (VA Code §19.2-70.3 is Virginia's version of 18 USC 2703.) Exceptions were added to the statute in situations where there is an administrative subpoena in a child pornography case and when there are emergency circumstances.

This bill was specifically geared towards the real-time location data of mobile telephones, whether through "pinging" the phone by an electronic communication service or through the use of the phone's internal GPS. While the location of the phone does not necessarily identify the location of the phone's owner, practical experience tells us that most of the time it does.

The 2014 amendments are in the italicized language as follows:

> C. *Except as provided in subsection D,* a provider of electronic communication service or remote computing service, including a foreign corporation that provides such services, shall disclose the contents of electronic communications *or real-time location data* to an investigative or law-enforcement officer only pursuant to a search warrant issued by a magistrate, a juvenile and domestic relations district court, a general district court, or a circuit court, based upon complaint on oath supported by an affidavit as required in § 19.2-54, or judicial officer or court of any of the several states of the United States or its territories, or the District of Columbia when the warrant issued by such officer or such court complies with the provisions of subsection G. In the case of a search warrant directed to a foreign corporation, the affidavit shall state that the complainant believes that the records requested are actually or constructively possessed by a foreign corporation that provides electronic communication service or remote computing service within the Commonwealth of Virginia. If satisfied that probable cause has been established for such belief and as required by Chapter 5 (§ 19.2-52 et seq.), the magistrate, the juvenile and domestic relations district court, the general district court, or the circuit court shall issue a warrant identifying those records to be searched for and commanding the person seeking such warrant to properly serve the warrant upon the foreign corporation.

D. A provider of electronic communication service or remote computing service, including a foreign corporation that provides such services, shall disclose a record or other information pertaining to a subscriber to or customer of such service, including real-time location data but excluding the contents of electronic communications, to an investigative or law-enforcement officer pursuant to an administrative subpoena issued pursuant to § 19.2-10.2 concerning a violation of § 18.2-374.1 or 18.2-374.1:1, former § 18.2-374.1:2, or § 18.2-374.3 when the information sought is relevant and material to an ongoing criminal investigation.

E. When disclosure of real-time location data is not prohibited by federal law, an investigative or law-enforcement officer may obtain real-time location data without a warrant in the following circumstances:

1. To respond to the user's call for emergency services;

2. With the informed, affirmative consent of the owner or user of the electronic device concerned if (i) the device is in his possession; (ii) the owner or user knows or believes that the device is in the possession of an employee or agent of the owner or user with the owner's or user's consent; or (iii) the owner or user knows or believes that the device has been taken by a third party without the consent of the owner or user;

3. With the informed, affirmative consent of the legal guardian or next of kin of the owner or user, if reasonably available, if the owner or user is reasonably believed to be deceased, is reported missing, or is unable to be contacted; or

4. If the investigative or law-enforcement officer reasonably believes that an emergency involving the immediate danger to a person requires the disclosure, without delay, of real-time location data concerning a specific person and that a warrant cannot be obtained in time to prevent the identified danger, and the possessor of the real-time location data believes, in good faith, that an emergency involving danger to a person requires disclosure without delay.

No later than three business days after seeking disclosure of real-time location data pursuant to this subsection, the investigative or law-enforcement officer seeking the information shall file with the appropriate court a written statement setting forth the facts giving rise to the emergency and the facts as to why the person whose real-time location data was sought is believed to be important in addressing the emergency.

J. A search warrant or administrative subpoena for the disclosure of real-time location data pursuant to this section shall require the provider to provide ongoing disclosure of such data for a reasonable period of time, not to exceed 30 days. A court may, for good cause shown, grant one or more extensions, not to exceed 30 days each.

K. For the purposes of this section:

"Electronic device" means a device that enables access to, or use of, an electronic communication service, remote computing service, or location information service, including a global positioning service or other mapping, locational, or directional information service.

"Real-time location data" means any data or information concerning the current location of an electronic device that, in whole or in part, is generated, derived from, or obtained by the operation of the device.

In a nutshell, these amendments resulted in the following:

- "Real time location data" may only be sought by law enforcement pursuant to a search warrant based on probable cause (or in the case of child pornography cases, pursuant to an administrative subpoena). This warrant is good for up to 30 days, with courts being authorized to grant additional 30 day extensions.

- Exceptions to this search warrant requirement include situations of emergencies, consent by a device's owner, consent by the next-of-kin of a missing person, or other exigent circumstances. If law enforcement invokes one of these emergency provisions, they must file with the court a written statement of the facts of the emergency.

Historic Cell-Tower Information

As drafters of this bill on real time location data, we specifically did not include "historic cell tower information." We subscribed to the United States Supreme Court's opinions which stated "an individual enjoys 'no legitimate expectation of privacy,' and so no Fourth Amendment protection, in information he "voluntarily turns over to a third party.' Smith v. Maryland, 442 U.S. 735, 743-44 (1979). This rule applies even when 'the information is revealed,' as it assertedly was here, 'on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.' United States v. Miller, 425 U.S. 435, 443 (1976)."

United States v. Graham, 796 F.3d 332, 378-79, (4th Cir. 2015)(J. Motz dissenting).

To a large degree, this was due to both the absence of simultaneously monitoring a person's present location and the lack of specificity in that location provided by cell tower information. While GPS can pinpoint location within feet, cell tower information is far less accurate with distances measured within thousands of feet, more or less. This technology is based on several factors relating to signal strength; including distance to tower, intervening objects between towers and the phone, the number of towers in the area and the number of calls a particular tower is handling.

2015

In 2015, Section 19.2-70.3 was further amended to include the requirement of a search warrant before law enforcement could use what is commonly referred to as a ***"sting ray."*** A "sting ray" is a fake cell phone tower used by law enforcement to locate cell phones.[1] "Sting Rays" were inadvertently left out of the 2014 legislation.

In 2015, there also were bills introduced in both chambers to limit the time period for the passive use of Automated License Plant Readers. These bills were debated extensively and modified many times. Ultimately, they passed the General Assembly as more expansive "surveillance technology" bills requiring a warrant. "Surveillance technology" was defined as "technology used to observe people, places or activities or to collect personal information, without the subject's knowledge or consent." Ultimately these bills were vetoed by Governor McAuliffe and were not reintroduced in the 2016 session, although the patrons have promised to raise the issue again in 2017 after further study.

United States v. Graham, 796 F.3d 332 (4th Cir. August 5, 2015)

On August 5, 2015, a three judge panel of the 4th Circuit Court of Appeals held that law enforcement's warrantless procurement of 221 days worth of historic cell tower information in the possession of electronic service providers to help prove that the defendants had participated in a string of robberies in Maryland was an unreasonable search in violation of the 4th Amendment. Historic cell tower information, although not as precise as GPS information, can be used to show generally the location of a mobile phone, and presumably the location of its owner.

However, because law enforcement acted in good faith on court orders (supported by less than probable cause) they obtained pursuant to the Electronic Communications Privacy Act and the Stored Communications Act, the Court held that the exclusionary rule did not apply in this case.

Specifically, the Court adopted the logic of the concurrence in United States v. Jones and held that "the government invades a reasonable expectation of privacy when it relies upon technology not in general use to discover the movements of an individual ***over an extended period of time***."

The 4th Circuit acknowledged that the 5th and the 11th circuits had reached the opposite conclusion concerning historic cell tower information. In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); United States v. Quartavious Davis, 785 F.3d 498 (11th Cir. 2015). However, the 4th Circuit refused to "accept the proposition that cell phone users volunteer to convey their location information simply by choosing to activate and use

[1] *Stingray, the Fake Cell Phone Tower Cops and Carriers Use to Track Your Every Move,* ExtremeTech, http://www.extremetech.com/mobile/184597-stingray-the-fake-cell-phone-tower-cops-and-providers-use-to-track-your-every-move, June 17, 2014.

their cell phones and to carry the devices on their person" because "[c]ell phone use is not only ubiquitous in our society today but, at least for an increasing portion of our society, it has become essential to full cultural and economic participation."

In November 2015, the 4th Circuit issued an order calling for a rehearing *en banc* in this case. That hearing is scheduled to take place on March 22, 2016.

Thank you for the opportunity to testify before you today, and I look forward to answering any questions the committee may have on this subject.